THE COALITION INFORMATION SYSTEMS AND OPERATIONS (CISO) LEARNING NETWORK: AN EMERGING CONCEPT FOR MULTINATIONAL C4 INTEROPERABILITY

Walter L. CHRISTMAN and Tom HAZARD

Introduction

Current and future military missions involve multi-national coalition forces that must be rapidly drawn together, flexibly led, responsively deployed and agile to address a wide variety of dynamically evolving tasks. Synchronization of air, land and sea campaigns will remain the cornerstone of Joint Operations as we move to confront the next generation of warfare. In all of these missions there is a need for agility, responsiveness and effectiveness in the use of limited resources to achieve complex and multiple objectives. Within this context, the primary challenges to effective integration of command, control, communications, and computers (C4) in attaining "Coalition Interoperability" and increased effectiveness are [1]:

- Different doctrine, decision making, rules of engagement and mission "agendas";
- Different technology skill and equipment levels;
- Questionable compatibility of respective national information systems;
- Limited information systems resource sharing agreements and capacity;
- Different interpretation of situational information;
- Lack of compatible security architectures.

To help address these challenges, the Coalition Information Systems and Operations (CISO) Learning Network is developing in collaboration with NATO and Partnership for Peace (PfP) nations an Internet-based online repository of e-Learning materials for enhanced coalition interoperability. Once fully implemented, it will promote net-centricity in coalition command and control through a global, Web-enabled environment that leverages existing and emerging technologies in a “smart-pull” fashion as part of the NATO transformation agenda.[2] For those wishing to certify their learning experiences for recognition and validation by national authorities, the CISO Learning Network is expected to include the award of a Coalition Information Officer Certificate by an appropriate NATO organization in collaboration with several potential nationally sponsored academic institutions. In addition, the CISO Learning Network can serve as a continuous education resource that will assist in guiding the planning and execution of combatant command strategy, as well as joint operations.

The next generation of warfare, often referred to as “fourth generation warfare,” will not only challenge the traditional views of how we operate “jointly” in the battle space, but will also greatly effect how we integrate those actions taken to affect adversary information and information systems, while defending coalition information and information systems. This new generation of warfare will shake the traditional warfighting concepts to the core and require all nations to fundamentally revisit current joint doctrinal philosophies on conducting joint operations and to seek new means for educating and training coalition forces.

The CISO Learning Network initiative is in response to the fact that Information Operations (IO), Information Warfare (IW) and Command and Control Warfare (C2W) may become the dominant operational and strategic weapons in combating nation-state or non-state actors, who may be engaging in destructive overt or provocative behavior. The identification of “coalition interoperability” has been deemed a critical success factor and one of the fundamental challenges to mission success in the post-Cold War security environment. It continues to rank as a top priority issue, as revealed in numerous internal US Defense Department after action reviews.

Moving beyond issues of technical interoperability, the CISO Learning Network addresses what might be called “cognitive interoperability.” Effective integration of C4 is a core competence and task among and between foreign militaries in addressing the challenge. The CISO Learning Network specifically addresses the problem of how to provide e-Learning capabilities (right time/right place educational opportunities, with on-demand potential) to a multinational audience. Primary target audiences include US and coalition personnel engaged in operational-level multinational command and staff tasks (e.g., Combined Joint Task Force). In addition, the CISO learning community includes a wider audience concerned with operational and strategic level C4 cooperation in a wide array of complex contingencies. It further covers the use of Information Assurance as a reliable enabler that should be included in the developing of Information Operations doctrine.

Fully developed, the CISO Learning Network will include:

- A permanent network dedicated to coalition forces and 'continuous learning';
- A SCORM "conformant" platform to support education and training on demand;
- A conduit for emerging advances in distributed learning & modeling and simulation;
- A means to build a global cooperative security community and to support it anytime, anywhere;
- Professional certification in collaboration with accredited academic institutions.

The CISO initiative's initial priority for content development is to focus on creating a sustainable learning environment that will allow the development of advanced 'critical thinking skills' in the Information Operations (IO) domain. The payoff will be improved technical and "human" interoperability between US military forces and their foreign counterparts, as well as a reduction in the OPTEMPO of US forces, as a consequence of improved performance among the planning staffs of a wide array of coalition partner nations. The end-result is expected to dramatically expand US and multinational learning opportunities in the domain areas of Coalition Information Operations (CIO) and planning for the Combined Joint Task Force (CJTF).

Getting Started

The initial impetus for the CISO Learning Network emerged in collaboration with experts from over 30 NATO and PfP nations at the US European Command Exercise *Combined Endeavor'02*. The Chairman of the NATO NC3 Board Working Group on Strategy and Policy, representing the Joint Staff J6, subsequently endorsed the CISO concept to the NATO Training Group as a promising pilot effort to improve coalition interoperability. The CISO Learning Network is the foundational database component of the C3 cooperative topic in the Partnership for Peace Information Management System (PIMS). The program's mission statement provides the overall guiding context for initial steps:

The Coalition Information Systems and Operations Learning Network will provide the essential familiarization of C4 planning skills necessary to integrate information technologies and command & control processes among and between NATO Allies and the Partnership for Peace nations.

As a prototype effort being tested within the NATO-PfP arena for eventual application worldwide, the CISO Learning Network is a joint project of the US Navy Space and Naval Warfare Systems Center - Charleston (SPAWAR SSC) and the

Naval Postgraduate School (NPS). A ‘prototype’ CISO knowledge portal has been established to administer the initial project at https://www.eur.spawar.navy.mil/ciso/. NPS Learning content borrowed with minor adaptation from previous investments by Naval Education and Training Command (NETC) for US Navy and Joint Service application is already under evaluation and being revised for coalition partners in the Euro-Atlantic region. A complete portal will be established as a result of funding to support development of a strategic plan and series of conferences and workshops involving PfP Partner and NATO representatives in the test and evaluation process. Foundation topics will include human interoperability, cognition and decision-making, command and control structures, joint planning process, and Information Operations (IO). All of the elements associated with IO are envisioned, including Information Warfare, Electronic Warfare, PSYOPs, Deception, OPSEC, Information Assurance, and Infrastructure Protection/Security.

To give further definition to the effort, the CISO Learning Network managers have adopted the following project goals:

- Develop with the C4 community of NATO and PfP nations an Internet-based online repository of e-Learning content/ materials to further C4 education opportunities and support enhanced coalition interoperability planning and exercises.
- Develop planning skills in support of the coalition command and control environment for future collaborative and coalition planning efforts based upon the CJTF concept.

At end state, the program will establish a full spectrum capability to support C4 distributed learning requirements throughout the Euro-Atlantic community of nations. The value to the European theater, and eventually other regional geographic Combatant Commands, will be the development of a better educated and trained cadre of coalition officers and civilians. These forces will better understand that the new battle space will be non-linear and more likely without definable boundaries, borders or battlefields. Success or failure in the Joint Operations arena will rely heavily on these newly educated forces and their efforts to ensure there is no insurmountable ‘fog of war’ by gaining the knowledge necessary to increase the effectiveness of joint operations through coalition interoperability across the C4 domain.

Principles for Establishing the CISO Learning Network

The CISO Learning Network is a “technology solution” to a coalition education and training need and should be aligned and implemented in accord with four basic principles [3]:

1. *"Focus on coalition-based interoperability."* US allies and partners need to shift their interoperability focus from one almost exclusively devoted to technical interoperability in favor of a balanced treatment of the technical, cognitive, organizational, doctrinal and "human" aspects of interoperability and multi-national cooperation.
2. *"Incorporate a 'transformational' perspective."* A "transformational" perspective accepts current baseline interoperability characteristics as the initial benchmark. This means that CISO's effective contribution is to help to establish the point of departure for national efforts for continuing coalition interoperability improvements.
3. *"Foster cooperation in C4I infrastructure."* Fostering cooperation in C4ISR research, development, and acquisition of systems, doctrine, and procedures for multinational operations will help ensure the transfer of "lessons learned" into the coalition partner's actual military capability.
4. "*Conduct experimental programs."* An experimental program, using different levels of complexity and reality (collaboration, war games, simulations, command post exercises, and true lessons learned efforts) CISO will ensure a process to build systematic and empirical knowledge about what actually works in multinational operations.

Focus on Coalition-Based Interoperability

The CISO Learning Network program is intended to provide participating nations with tangible measures and evidence of the benefits that can be expected from investments in coalition interoperability. To be effective, the CISO Learning Network program must:

- *Develop a common methodology*, which requires agreement with participants on the relevant representative mission areas (e.g., regional conflict, peacekeeping, and peace support operations) as well as the appropriate C4 interoperability learning objectives;
- *Build upon existing efforts*, which requires the application of web-based, Internet e-Learning technologies necessary to help counterpart foreign military organizations to "co-evolve" with US forces as part of the transformation experience. By taking advantage of existing laboratories, networks, and currently planned experiments, the CISO Learning Network may afford the initiation of a broadened interoperability effort with little added infrastructure costs to the participating nations;
- *Employ a cooperative process*, which will lay the foundation for enhanced security cooperation among the participating countries. In its implementation, NAVEUR and EUCOM employment of the CISO Learning

Network will be enable them to:

1. Take as the end-state goal with each individual partner nation a degree of joint responsibility in the co-evolution of operational concepts, command approaches, organizations, doctrine, and systems;
2. Incorporate other nations and non-governmental organizations as appropriate;
3. Foster a collective shared awareness and efficient, collaborative learning environment within which future coalition-based knowledge may be shared among and between all participants.

Incorporate a Transformational Perspective

The CISO Learning Network concept is based upon the assumption that Advanced Distributed Learning (ADL) through multinational education and training is a vital part of the *transformation* experience. NATO has already adopted ADL as its first priority project within the NATO Concept Development and Experimentation (CDE) arena. Therefore, as the NATO lead in this critical area of multinational education and training, the US is assured of participation in the co-evolution of a foreign nation's operational concepts, command approaches, organizations, doctrine, and systems. This program focuses on the *integration* of technology development efforts, organizational concepts, and doctrine development. E-Learning, employed through the CISO Learning Network program, is an essential part of the process of discovery, exploration, testing, assessment, and demonstration that are the engines of co-evolution in foreign military capability. The CISO Learning Network program will work best if it helps to facilitate the *transformation* of coalition education and training through the use of emerging technologies and over the Internet. Where required, it will incorporate and build upon existing initiatives with individual and systemic improvements in order to better achieve the theater-defined coalition-based training objectives.

Foster Cooperation in C4I Infrastructure

When building upon existing architecture, the emerging future architecture must be tailored to the needs of the nation or region with whom we are engaged. The following are among the range of specific technical solutions, which could be facilitated through the CISO Learning Network:

- Conduct multinational distributed computer-assisted exercises using high fidelity simulations;
- Collaborate in technical groups through the use of web-based technology services;

- Share lessons learned and knowledge resources through interconnected repositories of digital technical information;
- Increase interoperability through real time technical applications.

Conduct Experimental Programs

In support of conducting experimental programs, the CISO Learning Network program will provide a repository for lessons learned. Properly developed, it can serve as a clearinghouse for the continuing refinement of requirements and the continuing identification/ evaluation of viable technology. In order to take full advantage of all emerging technology and to ensure that the CISO concept is well positioned to optimize its value to the coalition forces, the CISO Learning Network will, as applicable:

- Capitalize on existing laboratories, networks, research networks and planned experiments where possible;
- Adopt a confederated approach to building the "system of systems" that will support a wide array of European C4 and IT platforms;
- Base interoperability on open systems architecture and de facto marketplace standards to the greatest extent possible, adding the military unique requirement only when essential;
- Undertake a program to assist foreign military officers better to understand emerging technologies and their significance.

Scoping the Effort and Defining the Task

In exploring CISO implementation, the US Navy SPAWAR and Naval Post Graduate School Team analyzed appropriate pedagogies, performance-based outcome measures and the overall efficacy of web-based learning. It was concluded that a properly developed 'anytime, anywhere' approach to delivering learning has the potential to substantially improve coalition interoperability by providing access to education across a "learning continuum" of the entire C4 requirement spectrum (i.e., in terms of content and audience). Specifically, Asynchronous Learning, through a variety of web-based tools, can provide a wide variety of 'anytime, anywhere' benefits while still accommodating the interactivity that may be required between faculty, instructors and learners. It was determined that the best approach to implementation would be the "crawl, walk, run" strategy carried out in three overlapping phases.

Phase I: Gap Analysis

Information Operations and Information Warfare (IO/IW) managers face infinite choices when they contemplate strategies for IO/IW applications and dealing with requisite changes in technology. Like the ‘private sector,’ if they do not know their destination, they may chose paths which are fraught with risk, or paths which lead to failure due to inadequate problem solving or decision making. It is essential then, that US and coalition leaders who plan to move from “here to there” in the IO/IW world are clear where “there” is. By knowing what the desired end state looks like, the leadership can compare that to the current state, identify the size and nature of the “gap” between the two, and take action to close the gap.

This first stage of the gap analysis was to evaluate the possibility of adapting the NPS IO content developed for US purposes to a coalition or multinational application. This required that all content domain factors be identified. With assistance from the Bulgarian Rakovsky Military Academy, the NATO School in Germany, and international students at NPS in Monterey, California, an initial gap analysis using NPS developed content is underway.

This process involves a highly interdisciplinary approach consisting of *foundational knowledge domains* drawn from several IO/IW areas of study. The resulting CISO Learning Network application is a baseline for coalition IO/C4 learning outcomes worldwide. It provides a foundation for further study in IO/C4 that will allow the coalition learners to be able to:

- Understand and create interoperable Information Operations strategies and policies;
- Understand and create agile organizational structures and decision processes responsive to real time mission and situation requirements;
- Understand information technology and systems as a provider of opportunities to gain information and knowledge superiority and perform information operations;
- Integrate technology, organization, policy and strategy into an Information Operations framework and use it in deliberate and crisis planning and execution across the range of military operations.

With respect to the ‘learning continuum,’ this gap analysis should aid in determining not only present needs but also serve to forecast future education needs based on emerging technologies or operational contingencies. The purpose of this ‘gap analysis’ process is to help ensure that institutional priorities are self-consciously factored into choices made related to the coalition IO/C4 courses. In identifying the types of training and education needed for the information officers of the workforce of the future, decisions must be made in areas such as:

- Type of courses;
- Number of courses;
- Delivery methods;

- Audience;
- Timing;
- Length;
- Sequence;
- Content.

Phase II: Course Development and Establishing a Community of Learners

With today's military environment being characterized by the emergence of assorted and complex contingencies, the requirement for effective multinational technical and 'human' interoperability has become increasingly apparent. Theater commanders are also finding that the inability of coalition partners to rapidly plan and coordinate with each other results in a default situation whereby the US forces must often become the lead responder in order to ensure success. Consequently, one objective of the CISO Learning Network is to certify the professional accomplishment of foreign military officers in acquiring C4 skills necessary to interoperate with US forces.

The SPAWAR/NPS team proposes to create a variety of learning modules/ courses, leading to professional development, certificate programs that are based upon a tightly knit set of coalition 'learning domains' resulting in a Coalition Information Officer (CIO) certificate. The first CIO modules would be an innovative education pursuit, which leverages the graduate degree program level content already being developed at NPS. Key domains areas to be examined are broken down into "knowledge domains" focused on general Information Operations issues and "problem domains" focused on practical application issues most likely to be faced within the coalition and multinational interoperability arena. Sub-elements of each are identified below.

The Foundational Knowledge Domains are:

Computer Technology
Networks
Information Assurance
Database Technology
Decision Support Systems and Artificial Intelligence
Sensor and Signal Processing
Communications Systems
Space Systems
Software Technology
Information Systems, Architectures, and Integration

Combat Systems
Probability and Statistics
Operations Analysis
Systems Evaluation
Information Operations
Command and Control
C4ISR Systems
Enterprise Integration
Mathematics

Example Information Operations Problem Domains are:

- Planning and Execution Processes
- Battle Staffs Decision Processes
- Psychological Operations
- Electronic Warfare
- Computer Network Attack
- Computer Network Defense
- Socio-Political Issues
- Command & Control Challenges
- Media
- Diplomacy
- Public Affairs
- Civil Affairs
- OPSEC / Deception

With assistance from the Bulgarian Rakovsky Military Academy, the NATO School, and International students from NPS, an initial set of 'pilot' web based Coalition Information Officer (CIO) modules have been completed and are ready for test and evaluation. In the web-based (online) version, learner engagement within these two major domains is largely asynchronous (anytime/anywhere), but not totally self-paced. Eventually, the online courses will feature access to a wide range of open source information resources, significant interactivity (faculty/student and peer/peer), substantial control of the learning environment by the individual coalition learner, and extensive modularization of content.

Phase III: Finalize and Maintain the CISO Learning Network

The development of a comprehensive international security cooperation e-Learning activity will also need to be supported by a coherent technology vision and strategy. Higher order capabilities are achieved by combining these basic user and content capabilities into interoperable and interacting systems. The following is a brief list of examples of higher order capabilities and systems. An infinite number of higher order capabilities are possible.

- *Traditional Learning Example*. To use the CISO Learning Network for learning, the student must find the appropriate course/ module, register for the course/ module, access the course content, provide information such as homework, papers, and exams, interact with the instructor, interact with other students, and track performance, progress, and status. Some opportunities for totally self-paced exploration will also be provided.

- *Teaching Example*. To use the CISO Learning Network for teaching, the instructor must develop the content, store the content, keep the content current, manage student enrollment, interact with the students, interact with other instructors, evaluate student performance, and track and report on student performance, progress, and status.
- *Digital Library and Reference Example*. To use the CISO Learning Network for accessing reference materials, the user must be able to find and access the desired content. This requires access functions such as search and discovery and retrieval. Also, the user may want to place certain content into one of the digital libraries. Here they may require creation and development functions, manipulation and modification functions, as well as access functions.
- *Distributed Simulation Example*. Because the CISO Learning Network is a Web-based system of capabilities, it would be possible for users to access and execute distributed simulations through the CISO portal itself. A properly integrated application interconnection from the portal to the distributed simulation system would be required. The users could then use the communication and collaboration functions provided by the CISO to contact each other and establish their parameters for a distributed simulation event.
- *Cooperative Security Community Example.* The CISO concept lends itself very well to establishing "communities of interest." In this example, users would use the communication and collaboration functions to contact other users to determine if they would be interested in forming a cooperative security community. Notices could be posted on the CISO learning network home page along with contact information for the organizers. The users establishing this community could develop content to stimulate and facilitate discussions. The users could establish on-line seminars and use the CISO portal knowledge pool to facilitate face-to-face events. This would become a community of people who could share ideas and concepts across many political borders.

It is clear from these examples that the functions already found in the CISO learning management system and digital libraries can be expanded and developed. Then it becomes a straightforward process to reuse them in these higher order systems. It is also clear from these examples that a properly integrated CISO Learning Network environment would provide a catalyst for developing an infinite number of higher order capabilities, limited only by imagination and bandwidth. These higher order and more complex capabilities would fuel further development of on-line communities and provide more opportunities for users across the globe to interact with, exchange, and create knowledge. The development of human interfaces and expanded functionality (e.g. multilingual, multi-sensory interface) greatly facilitates the use and accessibility of these high order systems.

Summary

The Coalition Information Systems and Operations Learning Network at fully developed end state is a web-based cooperative security forum or "knowledge portal" and, thus, by definition is an open-ended quest for intellectual and pedagogical modes of international cooperation. The benefit of an open system of knowledge is that it allows for wider participation in the processes of experimentation in which promising approaches to international security cooperation are subjected to the rigors of experimentation, simulations, gaming, exercises, and other forms of interaction. This methodology facilitates, among other things, the use of "test laboratories" to promote coalition interoperability and political-military cooperation.

It should be recognized that this entire process is predominantly about establishing a multinational learning community within an entirely new concept of international security cooperation. It incorporates emerging technologies in support of emerging concepts. The development process associated with the CISO Learning Network is therefore decidedly experimental in its approach. The CISO concept is to bring together NATO and PfP Partners, C4 educators, researchers, developers, and military professionals to jointly develop commonly agreed upon C4 educational approaches/ content leading to academic certification. Efforts focus on the integration of technology development efforts, organizational concepts, and doctrine development.

In summary, we believe the CISO Learning Network and the proposed Coalition Information Officer Certificate is a major step forward in recognizing the need for integrating, on a coalition and multinational basis, the essential component of knowledge centric people, adaptive organizations and architecture with doctrine, standards and networks. The process of creating and translating existing e-Learning courses developed for US purposes for a foreign, multinational purpose is not trivial and will involve the participation of IO/C4 domain experts and experienced e-Learning instructional designers from many nations around the world. The net-centric approach enables discovery, exploration, testing, assessment, and demonstration of transformational approaches co-developed with coalition partners.

With all the burdens attributed to operating in joint environment, providing requisite knowledge for coalition leaders to manage a volatile, rapidly changing C4 landscape—without losing sight of the Commanders Intent or Coalition objectives—is a challenge of the greatest magnitude. The CISO Learning Network concept provides another tool for meeting this challenge while also promoting cooperative development in multinational education and training as a vital part of the transformation imperative.

Notes:

[1] Among the key findings of the *International Workshop on Knowledge-Based Planning for Coalition Forces* (Artificial Intelligence Applications Institute, University of Edinburgh, 10-11 May 1999), <http://www.aiai.ed.ac.uk/project/coalition/ksco/ksco-1999/index.html> (14 April 2004). List derived from elements identified by Dr. LeRoy Pearce, Canadian Ministry of Defense.

[2] CISO technical concept supports the net-centric, edge-enabled vision best identified in David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age*, with a Foreword by John Stenbit (Washington, DC: DoD Command and Control Research Program, June 2003), <http://www.dodccrp.org/publications/pdf/Alberts_Power.pdf> (14 April 2004).

[3] These operational principles were developed in accordance with the recommendations outlined in the Report of a French-German-UK-U.S Working Group: *Coalition Military Operations: The Way Ahead Through Cooperability* (Arlington, VA: US-CREST, 2000).

WALTER CHRISTMAN is Director for Strategic Initiatives, Transformational Science and Technology (Code 61B) for the Space and Naval Warfare Systems Center, Charleston. He oversees the development and implementation of coalition-based distributed learning applications in the NATO and Partnership for Peace arena. *E-mail*: w.christman@gcsp.ch.

THOMAS HAZARD is the Director, Office of Continuous Learning at the Naval Postgraduate School (NPS) in Monterey, California. He oversees the development and provision of distributed learning content in support of a wide array of NPS courses and related activities. *E-mail*: trhazard@nps.edu.

Together, the authors are the joint program managers of the Coalition Information Systems and Operations Learning Network initiative.